#3
3-15-02

PATENT
81800.0179
Express Mail Label No. EL 713 632 464 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Yoshifumi TANIMOTO	Examiner: Not assigned
Serial No: Not assigned	
Filed: January 23, 2002	
For: EMAIL PROCESSING METHOD, EMAIL PROCESSING APPARATUS AND RECORDING MEDIUM	

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2001-017516 which was filed January 25, 2001, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 23, 2002

By: _____
Lawrence J. McClure
Registration No. 44,228
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 １月２５日

出願番号
Application Number: 特願２００１－０１７５１６

出願人
Applicant(s): 村田機械株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ８月２４日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　21791
【提出日】　平成13年 1月25日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
G06F 19/00
【発明の名称】　電子メール処理方法及び記録媒体
【請求項の数】　4
【発明者】
【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内
【氏名】　谷本　好史
【特許出願人】
【識別番号】　000006297
【氏名又は名称】　村田機械株式会社
【代表者】　村田　純一
【代理人】
【識別番号】　100078868
【弁理士】
【氏名又は名称】　河野　登夫
【電話番号】　06(6944)4141
【選任した復代理人】
【識別番号】　100114557
【弁理士】
【氏名又は名称】　河野　英仁
【電話番号】　06(6944)4141
【手数料の表示】
【予納台帳番号】　001889
【納付金額】　21,000円

出証特２００１－３０７４９０６

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子メール処理方法及び記録媒体

【特許請求の範囲】

【請求項１】　一以上の宛先が登録された宛先リストに対して電子メールを送信する電子メール処理方法において、前記宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成するステップと、生成した共通鍵を用いて暗号化したデータを含む電子メールを送信するステップとを含むことを特徴とする電子メール処理方法。

【請求項２】　一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信した場合、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成するステップと、生成した共通鍵を用いて前記暗号化データを復号するステップとを含むことを特徴とする電子メール処理方法。

【請求項３】　コンピュータに、一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成させるプログラムコード手段と、生成させた共通鍵を用いて暗号化したデータを含む電子メールを送信させるプログラムコード手段とを含むプログラムが記録してあることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項４】　一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信したコンピュータに、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成させ、生成させた共通鍵を用いて前記暗号化データを復号させるプログラムコード手段を含むプログラムが記録してあることを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えばメーリングリストを利用することにより、同一のデータを含む電子メールを複数の電子メールアドレスに対して送信する場合、またそのようにして送信された電子メールを受信した場合の電子メール処理方法、及びその方法を実施するための装置としてコンピュータを機能させる為のコンピュータプログラムが記録されている記録媒体に関する。

【０００２】

【従来の技術】

近年、コンピュータネットワークの急速な進展に伴い、安全なデータ通信を実現すべく、種々の暗号技術が注目されている。従来から、暗号化鍵及び復号鍵の両者の鍵が等しい暗号系である共通鍵暗号系、及び両者の鍵が異なる暗号系である公開鍵暗号系が広く利用されている。共通鍵暗号系の典型例としては米国商務省標準局が採用したＤＥＳ（Data Encryption Standards ）を、また公開鍵暗号系の典型例としてはＲＳＡ（Rivest Shamir Adleman ）を夫々挙げることができる。

【０００３】

一方、各ユーザの住所，氏名，電子メールアドレス等の個人を特定するＩＤ（Identity）情報を利用する暗号系が提案されている。この暗号系では、ＩＤ情報に基づいて送受信者間で共通の暗号化鍵を生成する。

【０００４】

このようなＩＤ情報に基づく暗号系であって、暗号文通信に先立って送受信者間での予備通信を必要としないものとして、ＩＤ－ＮＩＫＳ（ID-based non-interactive key sharing scheme ）が研究され提案されている。このＩＤ－ＮＩＫＳは、送受信者間で公開鍵，秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも不要であるので、任意のユーザ間で安全に通信を行うことができ、しかも、上述したように予備通信を必要としないので、ユーザの利便性が高いという利点を有している。そのため、将来の暗号系の中枢をなすものと期待されている。

【０００５】

図５はＩＤ－ＮＩＫＳのシステムの原理を示す説明図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共有鍵生成システムを構成している。図５において、エンティティＡのＩＤ情報は、ハッシュ関数ｈ（・）を用いてｈ（ＩＤＡ）で表す。センタは、任意のエンティティＡに対して、センタ公開情報｛ＰＣｉ｝、センタ秘密情報｛ＳＣｉ｝及びエンティティＡのＩＤ情報ｈ（ＩＤＡ）に基づいて、以下の如く秘密鍵ＳＡｉを計算し、エンティティＡへ配布する。

ＳＡｉ＝Ｆｉ（｛ＳＣｉ｝，｛ＰＣｉ｝，ｈ（ＩＤＡ））

【０００６】

エンティティＡは、他の任意のエンティティＢとの間に行う通信の暗号化および復号のための共通鍵ＫＡＢを、エンティティＡ自身の秘密鍵｛ＳＡｉ｝、センタ公開情報｛ＰＣｉ｝及びエンティティＢのＩＤ情報ｈ（ＩＤＢ）を用いて以下の如く生成する。

ＫＡＢ＝ｆ（｛ＳＡｉ｝，｛ＰＣｉ｝，ｈ（ＩＤＢ））

また、エンティティＢも同様にエンティティＡとの間で用いる共有鍵ＫＢＡを生成する。ＫＡＢ＝ＫＢＡの関係が常に成立するのであれば、共有鍵ＫＡＢ，ＫＢＡをエンティティＡ，Ｂ間で暗号化鍵および復号鍵として利用することができる。

【０００７】

上述したＩＤ－ＮＩＫＳを利用して電子メールの送受信を行う場合について説明する。まず、電子メールの送信者及び受信者は、自己の電子メールアドレス（ＩＤ情報）に基づいて定められた秘密鍵を予めセンタから夫々取得しておく。そして、送信者は、受信者の電子メールアドレス（ＩＤ情報）に基づいて生成された公開鍵と前記取得した秘密鍵とに基づいて共通鍵を生成し、生成した共通鍵を用いてデータを暗号化し、その暗号化したデータを電子メールにて送信する。一方、受信者は、送信者の電子メールアドレス（ＩＤ情報）に基づいて生成された公開鍵と前記取得した秘密鍵とに基づいて共通鍵を生成し、受信した電子メール中のデータを前記生成した共通鍵を用いて復号する。

【０００８】

このようにして暗号化及び復号を行うことにより、安全な電子メールの送受信を容易に実現することができる。なお、このようなＩＤ－ＮＩＫＳにおける暗号通信には、例えば上述したＤＥＳ等を用いることができる。

【０００９】

【発明が解決しようとする課題】

ところで、同一の電子メールを複数の宛先に対して送信する方法として、メーリングリストが広く利用されている。メーリングリストを利用する場合、メーリングリストを運営する電子メールサーバにより、そのメーリングリストに予め登録されている電子メールアドレスに対して電子メールが同報配信される。その結果、複数の利用者が同一の電子メールを受信することができる。

【００１０】

しかしながら、ＩＤ－ＮＩＫＳにおいては、上述したように送信者は自己の秘密鍵及び受信者の電子メールアドレスを用いてデータを暗号化する必要があるので、複数の受信者に同一の電子メールを送信するときであっても、それら受信者の電子メールアドレス夫々を用いてデータの暗号化を実行し、暗号化したデータを含む各電子メールを夫々送信しなければならず、上述したようなメーリングリストを利用することはできないという問題があった。

【００１１】

本発明は斯かる事情に鑑みてなされたものであり、メーリングリスト等の一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成し、その共通鍵を用いて暗号化したデータを含む電子メールを送信し、一方この電子メールを受信した場合、宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成し、その共通鍵を用いて受信した電子メールに含まれているデータを復号することによって、宛先が複数ある場合における暗号化したデータを含む電子メールの送受信を容易に行うことができる電子メール処理方法、及びその方法を実施するための装置としてコンピュータを機能させる為のコンピュータプログラムが記録されている記録媒体を提供することを目的とする。

【００１２】

【課題を解決するための手段】

第１発明に係る電子メール処理方法は、一以上の宛先が登録された宛先リストに対して電子メールを送信する電子メール処理方法において、前記宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成するステップと、生成した共通鍵を用いて暗号化したデータを含む電子メールを送信するステップとを含むことを特徴とする。

【００１３】

第２発明に係る電子メール処理方法は、一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信した場合、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成するステップと、生成した共通鍵を用いて前記暗号化データを復号するステップとを含むことを特徴とする。

【００１４】

第３発明に係る記録媒体は、コンピュータに、一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成させるプログラムコード手段と、生成させた共通鍵を用いて暗号化したデータを含む電子メールを送信させるプログラムコード手段とを含むプログラムが記録してあることを特徴とする。

【００１５】

第４発明に係る記録媒体は、一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信したコンピュータに、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成させ、生成させた共通鍵を用いて前記暗号化データを復号させるプログラムコード手段を含むプログラムが記録してあることを特徴とする。

【００１６】

第１発明及び第３発明による場合、例えばメーリングリスト等のように、一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵と、電子メールを送信する送信元の電子メールアドレスに基づいて生成された秘密鍵とを用いて共通鍵を生成し、その生成した共通鍵を用いて送信対象であるデータを暗号化した後にその暗号化したデータを含む電子メールを送信する。

【００１７】

これにより、複数の電子メールアドレスに対して電子メールを送信する場合であっても、それらの電子メールアドレス夫々に基づいて暗号化したデータを含む各電子メールを夫々送信する必要はなく、それらの電子メールアドレスが登録されている宛先リストの電子メールアドレスを用いて暗号化を実行し、その結果暗号化されたデータを含む一の電子メールを送信するだけで足りる。よって、暗号化されたデータを含む電子メールを複数の宛先に対して容易に送信することができる。

【００１８】

第２発明及び第４発明による場合、一以上の宛先が登録された宛先リスト宛に送信された暗号化データを含む電子メールを受信した場合、宛先リストの電子メールアドレスに基づいて生成された秘密鍵と、電子メールを送信した送信元の電子メールアドレスに基づいて生成された公開鍵とを用いて共通鍵を生成し、その生成した共通鍵を用いて受信した電子メールに含まれている暗号化データを復号する。

【００１９】

これにより、一以上の宛先が登録された宛先リスト及び電子メールの送信元夫々の電子メールアドレスを用いて生成された共通鍵により暗号化されたデータを容易に復号し、内容を確認することができる。

【００２０】

【発明の実施の形態】

以下、本発明をその実施の形態を示す図面に基づいて詳述する。

図１は、本発明の電子メール処理方法を実施するための装置として機能するパ

ーソナルコンピュータPC1,PC2,…,PCn（ｎは自然数）と、これらのパーソナルコンピュータPC1,PC2,…,PCnが接続されているコンピュータネットワークとの構成例を示すブロック図である。

【００２１】

図１において、NTW はコンピュータネットワークであるインターネットを示しており、このインターネットNTW には、インターネットNTW への接続業者である多数のプロバイダPR1,PR2,…,PRn（ｎは自然数）が接続されている。

【００２２】

プロバイダPR1,PR2,…,PRnは、これらと契約したクライアントに対して電子メールの送受信サービスを提供する電子メールサーバとして機能するサーバSV1,SV2,…,SVn（ｎは自然数）を夫々備えている。

【００２３】

またプロバイダPR1,PR2,…,PRnのサーバSV1,SV2,…,SVnには、ルータRT1,RT2,…,RTn（ｎは自然数）及びアナログ回線Ｌを介してクライアントとしてのパーソナルコンピュータPC1,PC2,…,PCnが夫々接続されている。なお、ルータRT1,RT2,…,RTnに代えて、公衆電話回線の交換機を用いてもよい。

【００２４】

センタＣは、秘密鍵として機能する第１秘密鍵PRK1-1,PRK1-2,…, PRK1-nを各ユーザに対して夫々発行する。これらの第１秘密鍵PRK1-1,PRK1-2,…, PRK1-nは、各ユーザが利用する電子メールアドレスに基づいて夫々定められており、電子メール等の手段を用いて各パーソナルコンピュータPC1,PC2,…,PCnへ夫々送信される。

【００２５】

またセンタＣは、同じく秘密鍵として機能する第２秘密鍵PRK2をメーリングリストに対して発行する。この第２秘密鍵PRK2は、メーリングリストの電子メールアドレスに基づいて定められており、電子メール等の手段を用いて、そのメーリングリストを運営する電子メールサーバ（以下、ＭＬサーバという）MSへ送信される。

【００２６】

ＭＬサーバMSは、上述したようにしてセンタＣから受信した第２秘密鍵PRK2を含む電子メールを、メーリングリストに登録されている電子メールアドレス宛に送信する。これにより、各パーソナルコンピュータPC1,PC2,…,PCnは第２秘密鍵PRK2を取得することができる。

【００２７】

なお、各パーソナルコンピュータPC1,PC2,…,PCnがセンタＣから第１秘密鍵PRK1を又はＭＬサーバMSから第２秘密鍵PRK2を夫々取得する方法、またＭＬサーバSV3 がセンタＣから第２秘密鍵PRK2を取得する方法としては、上述した電子メールを利用する以外にも、例えばそれらの秘密鍵を記憶させたフレキシブルディスクを郵送等の手段により受け取ることによって取得するようにしてもよい。

【００２８】

さらに、ネットワークNTW には、データベースサーバDSが接続されている。このデータベースサーバDSは、本発明に係る電子メール送信装置のプログラムを記録している記録媒体DBを備えている。

【００２９】

図２は、本発明の電子メール処理方法を実施するための装置として機能するパーソナルコンピュータPC1 の構成を示すブロック図である。なお、パーソナルコンピュータPC2,…,PCnの構成は、パーソナルコンピュータPC1 の場合と同様であるので説明を省略する。

図２において、１はＣＰＵ及びキャッシュメモリ等で構成される制御部であり、該制御部１は、バス８を介して接続された各ハードウェア各部を制御すると共に、後述するハードディスク４に記憶されている種々のコンピュータプログラムを実行する。

【００３０】

ＲＡＭ２は、ＳＲＡＭ又はＤＲＡＭ等で構成され、制御部１において発生した一時的なデータを記憶する。

【００３１】

外部記憶装置３は、ＣＤ－ＲＯＭドライブ又はフレキシブルディスクドライブ等で構成され、本発明の電子メール送信方法及び電子メール処理方法に係るプロ

グラムが記録されているＣＤ－ＲＯＭ又はフレキシブルディスク等の可搬型記録媒体１０から前記プログラムを読み取る。

【００３２】

ハードディスク４は、読み書き可能な磁気ディスクから構成され、外部記憶装置３により読み取った本発明の電子メール装置のプログラム、及びパーソナルコンピュータPC1 の動作に必要な種々のコンピュータプログラムを記憶する。

【００３３】

また、このハードディスク４は、上述したようにしてセンタＣから取得した第１秘密鍵PRK1-1及び第２秘密鍵PRK2を記憶している。

【００３４】

なお、図２はパーソナルコンピュータPC1 の構成を示しているため、ハードディスク４は第１秘密鍵PRK1-1を記憶しているが、パーソナルコンピュータPC2,…,PCnの場合、ハードディスク４は第１秘密鍵PRK1-2，…，PRK1-nを夫々記憶している。

【００３５】

また、後述するように、第１秘密鍵PRK1-1は電子メールを送信する場合に用いられ、また第２秘密鍵PRK2はメーリングリストに係る電子メールを受信する場合に用いられる。したがって、パーソナルコンピュータPC1 が電子メールを送信するのみであって、メーリングリストに係る電子メールを受信することがない場合は、第２秘密鍵PRK2がハードディスク４に記憶されていなくてもよい。

【００３６】

モデム５は、インターネットNTW を介してデータ通信を行うための通信インタフェースであり、アナログ回線Ｌとの閉結及び解放の動作を行う。なお、モデム５の代わりに、ＤＳＵ（Digital Service Unit）を用いることにより、ベースバンド伝送方式のデジタル回線と接続するようにしてもよい。

【００３７】

表示部６は、ＣＲＴディスプレイ又は液晶表示装置（ＬＣＤ）等の表示装置であり、パーソナルコンピュータPC1 の動作状態を表示したり、種々の入出力データの表示を行う。また、操作部７は、パーソナルコンピュータPC1 を操作するた

めに必要なキーボード等の入力装置である。

【００３８】

なお、本発明の電子メール処理方法に係るプログラムは、上述したようにして可搬型記録媒体１０から読み取る以外にも、インターネットNTW を介して上述したデータベースサーバDSに接続し、このデータベースサーバDSが備えている記録媒体DBからパーソナルコンピュータPC1 へ前記プログラムをダウンロードすることができる。そして、そのダウンロードしたプログラムをハードディスク４に記憶し、記憶したプログラムを制御部１がＲＡＭ２にロードすることによって、パーソナルコンピュータPC1 は後述する処理を実行することができる。

【００３９】

次に、パーソナルコンピュータPC1,PC2,…,PCnの動作について説明する。

図３は、パーソナルコンピュータPC1 がメーリングリスト宛に電子メールを送信する場合の制御部１の処理手順を示すフローチャートである。なお、パーソナルコンピュータPC1 は、接続契約をしているプロバイダPR1 に対してユーザＩＤ，パスワード等を送出することによりログインしているものとする。

【００４０】

ＭＬサーバMSが運営しているメーリングリストに参加しているユーザは、操作部７を操作することにより、電子メールの宛先である前記メーリングリストの電子メールアドレスを入力し、また電子メールにて送信するデータを入力する。そして、ユーザは、その電子メールの送信をパーソナルコンピュータPC1 に対して指示する。

【００４１】

パーソナルコンピュータPC1 が備える制御部１は、電子メールの送信指示をユーザから受け付けた場合、上述したようにして入力されたメーリングリストの電子メールアドレスに基づいて定められた公開鍵及びハードディスク４に記憶されている第１秘密鍵PRK1-1を読み込む（Ｓ１１）。

【００４２】

次に、ステップＳ１１にて読み込んだ公開鍵及び第１秘密鍵PRK1-1を用いて共通鍵を生成する（Ｓ１２）。そして、このようにして生成した共通鍵を用いて、

上述したようにして入力された送信対象のデータを暗号化する（Ｓ１３）。

【００４３】

次に、上述したようにして入力されたメーリングリストの電子メールアドレスを宛先に設定し、ステップＳ１３にて暗号化したデータを用いて電子メールを作成し（Ｓ１４）、作成した電子メールを送信する（Ｓ１５）。

【００４４】

このようにしてパーソナルコンピュータPC1 から送信された電子メールは、サーバSV1 を介してＭＬサーバMSによって受信される。そして、ＭＬサーバMSは、パーソナルコンピュータPC1 から受信した電子メールをメーリングリストに登録されている電子メールアドレス宛に同報送信する。

【００４５】

図４は、パーソナルコンピュータPC2,…,PCnがメーリングリストに係る電子メールを受信した場合の制御部１の処理手順を示すフローチャートである。なお、パーソナルコンピュータPC2,…,PCnは、接続契約をしているプロバイダPR2,…,PRnに対してユーザＩＤ，パスワード等を送出することにより夫々ログインしているものとする。

【００４６】

ＭＬサーバMSが運営しているメーリングリストに参加している各ユーザは、パーソナルコンピュータPC2,…,PCnに対して電子メールを受信するように指示する。パーソナルコンピュータPC2,…,PCnが備える制御部１は、電子メールの受信指示をユーザから受け付けた場合、上述したようにしてＭＬサーバMSから送信されたメーリングリストに係る電子メールをサーバSV2,…,SVnから受信し、その受信した電子メールを読み込む（Ｓ２１）。

【００４７】

次に、ハードディスク４に記憶されている第２秘密鍵PRK2を読み込む（Ｓ２２）。そして、その読み込んだ第２秘密鍵PRK2とステップＳ２１にて読み込んだ電子メールの送信者の電子メールアドレスに基づいて生成された公開鍵とを用いて、共通鍵を生成し（Ｓ２３）、生成した共通鍵を用いて前記受信した電子メールのデータを復号する（Ｓ２４）。

【００４８】

これにより各ユーザはメーリングリストに係る暗号化された電子メールの内容を確認することができる。

【００４９】

なお、本実施の形態ではメーリングリストを利用して電子メールの送受信を行っているが、メーリングリスト以外であっても、一の電子メールアドレスを宛先とした場合に複数の宛先に対して同一の電子メールを同報送信することができる仕組みであれば、本発明を適用することが可能である。

【００５０】

【発明の効果】

以上詳述した如く、本発明によれば、メーリングリスト等の一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された共通鍵により共通鍵を生成し、その共通鍵を用いて暗号化したデータを含む電子メールを送信し、一方この電子メールを受信した場合、宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成し、その共通鍵を用いて受信した電子メールに含まれているデータを復号することによって、宛先が複数ある場合における暗号化したデータを含む電子メールの送受信を容易に行うことができる等、本発明は優れた効果を奏する。

【図面の簡単な説明】

【図１】

本発明の電子メール処理方法を実施するための装置として機能するパーソナルコンピュータと、これらのパーソナルコンピュータが接続されているコンピュータネットワークとの構成例を示すブロック図である。

【図２】

パーソナルコンピュータの構成を示すブロック図である。

【図３】

パーソナルコンピュータがメーリングリスト宛に電子メールを送信する場合の制御部の処理手順を示すフローチャートである。

【図４】

パーソナルコンピュータがメーリングリストに係る電子メールを受信した場合の制御部の処理手順を示すフローチャートである。

【図５】

ＩＤ－ＮＩＫＳのシステムの原理を示す説明図である。

【符号の説明】

１　制御部

２　ＲＡＭ

３　外部記憶装置

４　ハードディスク

５　モデム

６　表示部

７　操作部

Ｃ　センタ

MS　メーリングリストサーバ

NTW　インターネット

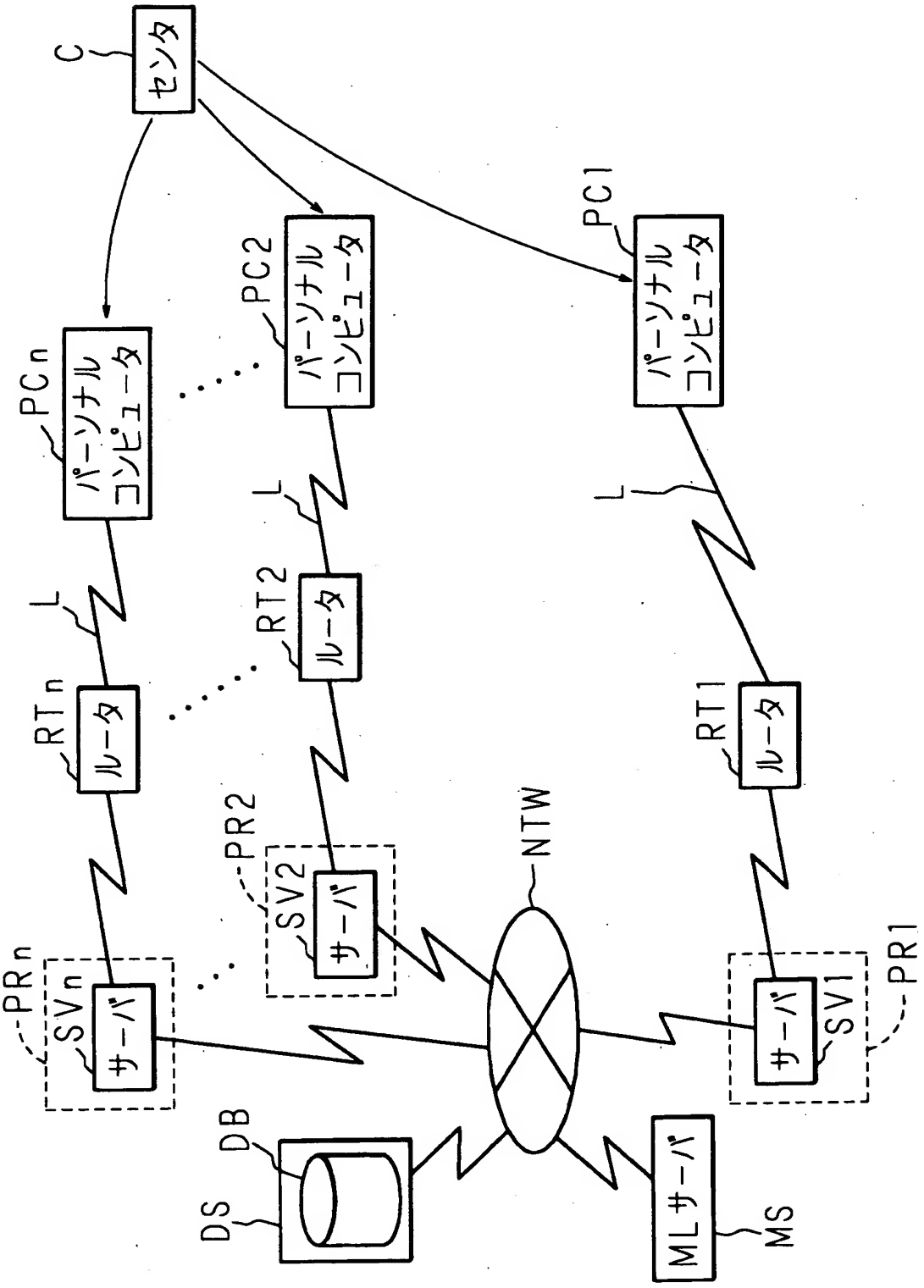
PC1,PC2,…,PCn　パーソナルコンピュータ

PRK1-1　第１秘密鍵

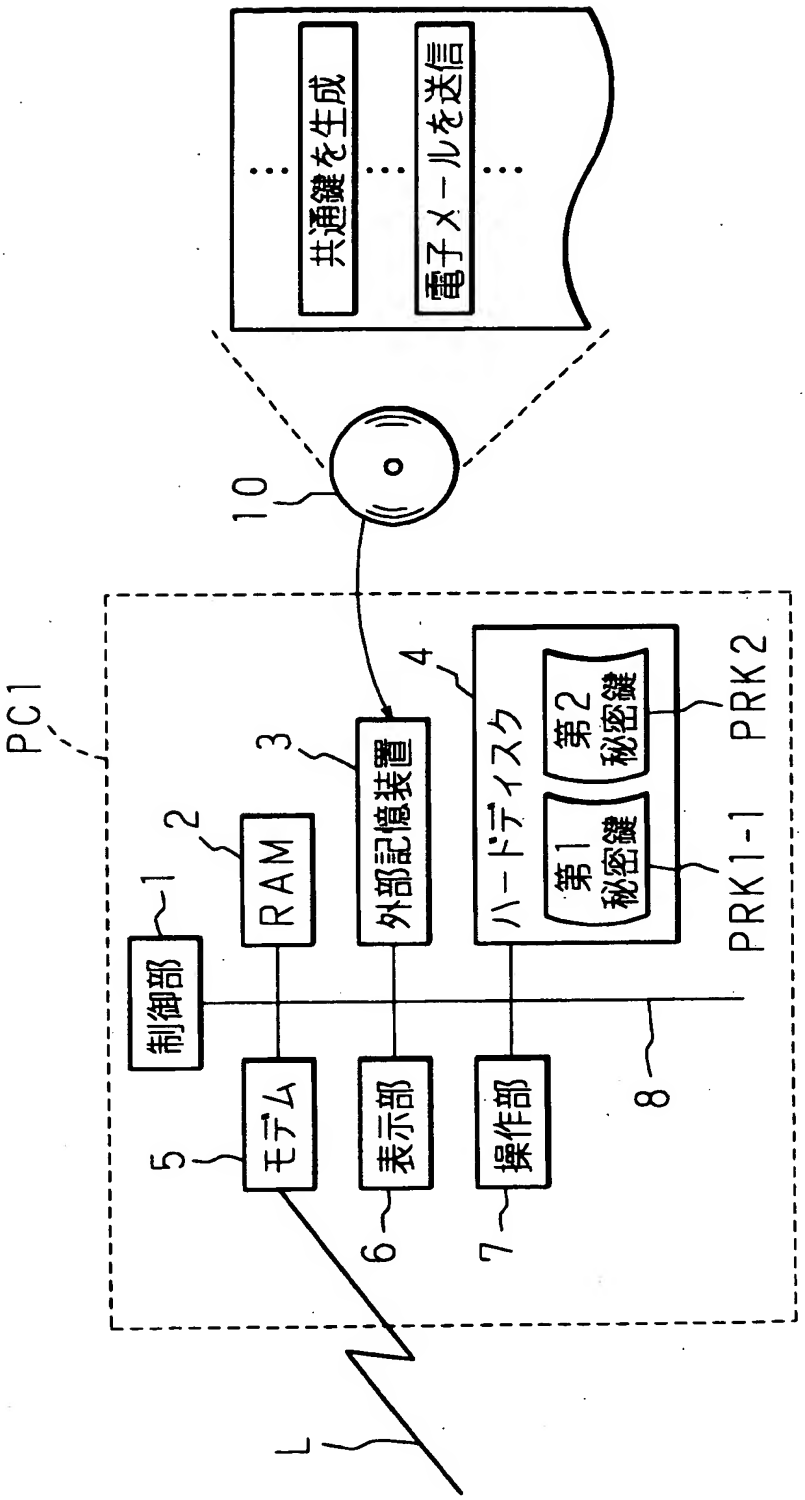
PRK2　第２秘密鍵

【書類名】　　図面

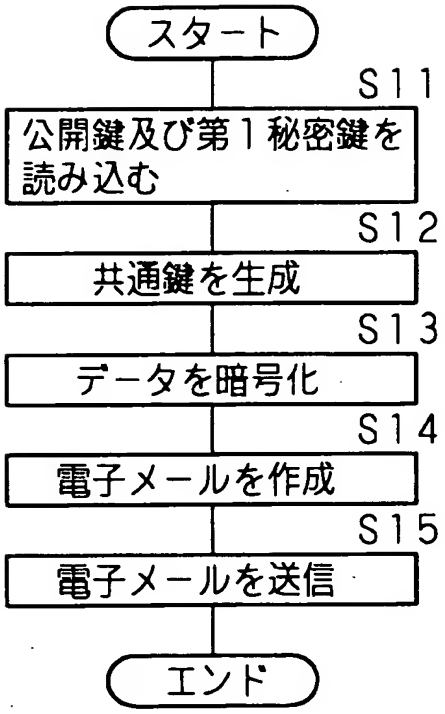
【図１】


C
センタ
PC1
パーソナル
コンピュータ
PC2
パーソナル
コンピュータ
PCn
パーソナル
コンピュータ
L
L
L
RT1
ルータ
RT2
ルータ
RTn
ルータ
PR1
SV1
サーバ
PR2
SV2
サーバ
PRn
SVn
サーバ
NTW
DB
DS
MLサーバ
MS

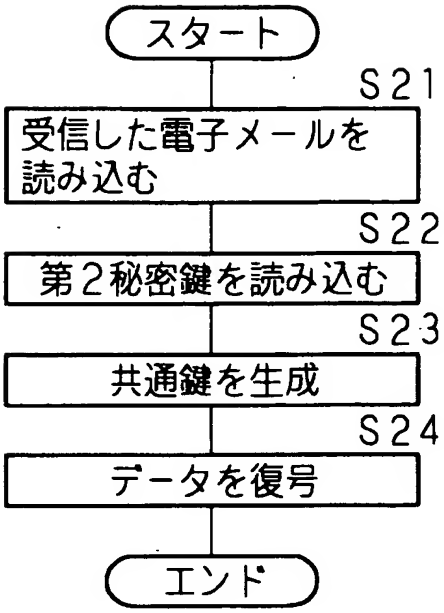
【図２】


共通鍵を生成
電子メールを送信
10
PC1
3
外部記憶装置
4
ハードディスク
第2秘密鍵
PRK2
第1秘密鍵
PRK1-1
2
RAM
1
制御部
5
モデム
6
表示部
7
操作部
8
L

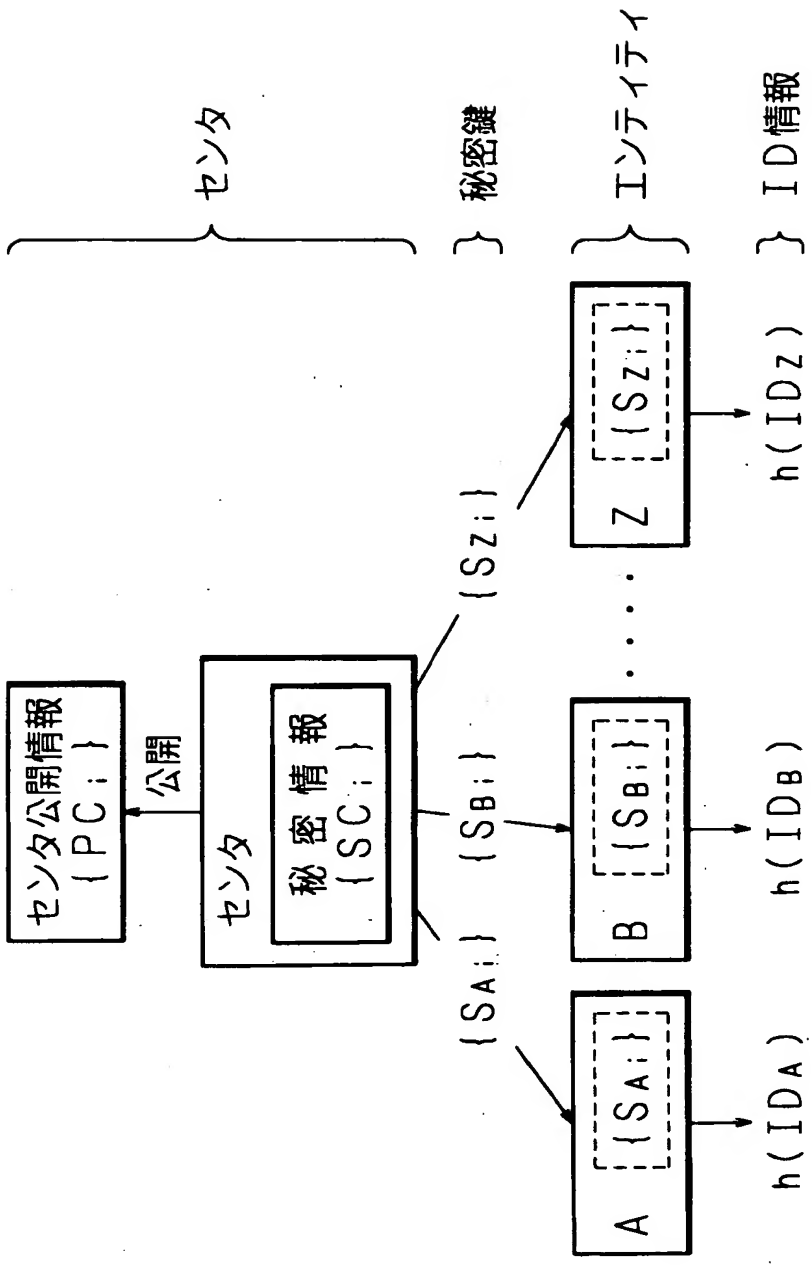
【図３】


スタート
S11
公開鍵及び第１秘密鍵を読み込む
S12
共通鍵を生成
S13
データを暗号化
S14
電子メールを作成
S15
電子メールを送信
エンド

【図４】


スタート
S21
受信した電子メールを読み込む
S22
第２秘密鍵を読み込む
S23
共通鍵を生成
S24
データを復号
エンド

【図５】


センタ
秘密鍵
エンティティ
ID情報
センタ公開情報
{PCi}
公開
センタ
秘密情報
{SCi}
{SZi}
{SBi}
{SAi}
Z
{SZi}
B
{SBi}
A
{SAi}
h(IDZ)
h(IDB)
h(IDA)

【書類名】　　要約書

【要約】

【課題】　暗号化されたデータを含む電子メールを効率的に同報送信することができる電子メール処理方法及び記録媒体の提供。

【解決手段】　パーソナルコンピュータPC1 は、メーリングリストを宛先とした電子メールの送信指示をユーザから受け付けた場合、そのメーリングリストの電子メールアドレスに基づいて生成された公開鍵及び予めセンタから取得した秘密鍵を用いて共通鍵を生成し（Ｓ１２）、生成した共通鍵を用いて送信対象のデータを暗号化する（Ｓ１３）。そして、その暗号化したデータを含む電子メールをメーリングリスト宛に送信する（Ｓ１５）。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社